

Abstract of the Disclosure

A context-aware firewall and intrusion detection system receives a definition of a Protocol State Machine (PSM) that defines the expected behavior of any protocol (FTP, HTTP, etc.). The PSM provides rules for detecting flows that deviate from the defined protocol behavior and taking appropriate actions. PSMs are comprised of rule groups that define behavior of a protocol. The rules include conditions and actions that may be executed if the conditions are satisfied. The actions include dynamically adding filters to be applied to the network flow, saving results for use in later executed rules, and activating and deactivating rules. Thus, these firewalls are capable of selective and intelligent processing based on flow state information and control payload.

"Express Mail" mailing label number: EV415949631US
Date of Deposit: March 31, 2004
This paper or fee is being deposited on the date indicated above with the United States Postal Service pursuant to 37 CFR 1.10, and is addressed to the Commissioner for Patents, Mail Stop Patent Application, P.O. Box 1450, Alexandria, VA 22313-1450.